1

;UMENTATION PAGE

Form Approved
OMB No. 0704-0188

ated to average 1 hour per response. including the time for reviewing instructions, searching existing data sources, gathering and ollection of information Send comments regarding this burden estimate or any other aspect of this collection of information including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188), Washington, DC 20503

1 AGENCY USE ONLY *(Leave blank)*

2 REPORT DATE
December 1990

3 REPORT TYPE AND DATES COVERED
Presentation/paper

4 TITLE AND SUBTITLE
SAFENET II—THE NAVY'S FDDI-BASED COMPUTER NETWORK STAND 'RD

5 FUNDING NUMBERS
PR: CC86
WU: DN088 539
PE: SCN

6 AUTHOR(S)
J. L. Paige and E. A. Howard

7 PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
Naval Ocean Systems Center
San Diego, CA 92152-5000

8 PERFORMING ORGANIZATION REPORT NUMBER

9 SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)
Naval Sea Systems Command
Washington, DC 20362

10 SPONSORING/MONITORING AGENCY REPORT NUMBER

11 SUPPLEMENTARY NOTES

12a DISTRIBUTION/AVAILABILITY STATEMENT

Approved for public release; distribution is unlimited.

12b DISTRIBUTION CODE

13 ABSTRACT *(Maximum 200 words)*

-- The SAFENET II (Survivable Adaptable Fiber Optic Embedded Network) standard is a seven layer profile which is being developed for use in Navy computer networks. SAFENET II employs the ANSI FDDI standard as its physical and data link layers. The profile also includes protocols from OSI and MAP, as well as the emerging Xpress Transfer Protocol (XTP). The SAFENET II profile is broken down into three protocol suites: OSI, lightweight, and combined. Any of these suites may be implemented depending on the system requirements. The SAFENET II physical topology is adapted from the FDDI standard, and includes the use of bypass switches for enhanced reliability. SAFENET II provides many network survivability features to the system integrator.

Published: *Proceedings* SPIE OE/Fibers 1990, V. 1364, September 1990.

14 SUBJECT TERMS
computer
display systems
data transmission

15 NUMBER OF PAGES

16 PRICE CODE

17 SECURITY CLASSIFICATION OF REPORT	18 SECURITY CLASSIFICATION OF THIS PAGE	19 SECURITY CLASSIFICATION OF ABSTRACT	20 LIMITATION OF ABSTRACT
UNCLASSIFIED	UNCLASSIFIED	UNCLASSIFIED	SAME AS REPORT

SAFENET II - The Navy's FDDI-based computer network standard

Jeffrey L. Paige and Edward A. Howard

Naval Ocean Systems Center
San Diego, CA 92152

ABSTRACT

The SAFENET II standard is a seven layer network profile which is being developed for use in Navy computer networks. SAFENET II employs the ANSI FDDI standard as its physical and data link layers. The profile also includes protocols from OSI and MAP, as well as the emerging Xpress Transfer Protocol (XTP). The SAFENET II profile is broken down into three protocol suites: OSI, lightweight, and combined. Any of these suites may be implemented depending on the system requirements. The SAFENET II physical topology is adapted from the FDDI standard, and includes the use of bypass switches for enhanced reliability. SAFENET II provides many network survivability features to the system integrator.

1. INTRODUCTION

The SAFENET (Survivable Adaptable Fiber Optic Embedded Network) program is an effort by the US Navy to develop standard computer network profiles which meet the requirements of Navy shipboard mission critical computer systems[1]. The SAFENET standards are the product of a joint Navy-industry working group which works in open forum to achieve consensus on all technical issues.

1.1 The SAFENET standards

There are two SAFENET standards currently in development, SAFENET I and SAFENET II. Each of these standards defines a computer network profile which includes a commercial local area network (LAN). Each SAFENET standard is based on existing and proposed commercial network standards to reduce development time and cost, and to permit the use of commercial components whenever possible.

The distinction between the two SAFENET standards is limited to the specific commercial LAN standard which each is based upon. SAFENET I is based on the IEEE 802.5 token-ring LAN[2] with a specified data rate of 16 Mb/s. This standard is considered suitable for Navy computer systems with moderate data throughput requirements. SAFENET II is based on the ANSI FDDI LAN[3-6] which operates at 100 Mb/s. The SAFENET II standard is intended for Navy computer systems which either have high data throughput requirements now, or else need to be designed to support such requirements in the future. The remaining portions of the standards, including ISO layers 3 through 7 and the physical medium specification, are identical. The remainder of this paper discusses the SAFENET II standard.

1.2 SAFENET II features

The SAFENET II standard will provide a Navy systems integrator with a number of significant features. In particular, the interconnectivity provided by a network is likely to be essential in future systems, as well as being a highly desirable upgrade to existing systems which are currently point-to-point interfaced. Another important feature of SAFENET II is its use of a fiber optic transmission medium. The insensitivity of fiber optics to electromagnetic interference is particularly advantageous for a system operating in the extremely noisy electromagnetic environment of a Navy ship.

SAFENET II contributes to system survivability as well by providing automatic fault isolation and reconfiguration mechanisms. These features are provided as a functions of the FDDI LAN standard. In addition, the SAFENET II standard permits a great degree of implementation flexibility. For example, a SAFENET II interface could be implemented either as an embedded interface within a host computer, or as a stand-alone interface unit to which devices can be connected. Finally, SAFENET II is based primarily on commercial standards and does not require any proprietary technology. Therefore, it should be possible for the Navy to obtain SAFENET II compliant networks and components from different vendors.

2. THE SAFENET II PROFILE

SAFENET II employs a layered protocol architecture which is based on the OSI reference model for computer networks[7,8]. Within this layered architecture SAFENET II specifies one or more protocols at each layer. The complete set of specified protocols is known as the SAFENET II profile.

The SAFENET II communications architecture divides the protocol profile into three service partitions, each of which constitutes a portion of the seven layer ISO reference model. These partitions are called user services, transfer services, and local area network (LAN) services. The SAFENET II service partitions are not intended to provide any implementation guidance. Rather, they are used to split the full profile into manageable parts with distinctly different requirements. These service partitions, the communication protocols they include, and their relationship to the ISO reference model are shown in Figure 1 for the SAFENET II profile. Note that the physical medium falls outside the ISO model and is therefore not considered part of the LAN services partition.

The user services partition corresponds to the application, presentation, and session layers of the ISO model (layers 5-7). These services provide the user with the capability to interact with, manage, and respond to the underlying transfer services. Below this, the transfer services partition corresponds to the transport and network layers of the ISO model, as well as the logical link control sublayer of the data link layer (layers 2-4). These services provide reliable communication mechanisms to the network user. Finally, the LAN services partition corresponds to the medium access control sublayer of the data link layer, as well as the physical layer of the ISO model (layers 1-2). The LAN services consist of those provided by the FDDI local area network, that is, the ability to get data on and off the physical medium in a controlled manner.

3. PROTOCOL SUITES

The SAFENET II communications architecture can also be separated into its distinct implementation classes, called protocol suites. These suites define the only implementation classes permitted by the SAFENET II standard. There are three such suites: the OSI protocol suite, the lightweight protocol suite, and the combined protocol suite. In addition to these suites, the SAFENET II profile includes some protocols and services which are common to all protocol suite implementations. These protocol suites, the communication protocols they include, and the communication protocols common to all suites are shown in Figure 2. Note that the combined protocol suite is not shown as a distinct entity, since it is the union of the OSI and lightweight suites.

3.1 OSI protocol suite

The OSI protocol suite provides full OSI compliant networking to systems which require it. This suite specifies the use of the Manufacturing Automation Protocol (MAP), version 3.0[9]. At the application layer, the MAP File Transfer, Access, and Management (FTAM) protocol is specified. Within the transfer services partition the ISO connection-oriented transport protocol - class 4 (TP4) is required[10]. These protocols are intended to provide communications interoperability in an open systems environment.

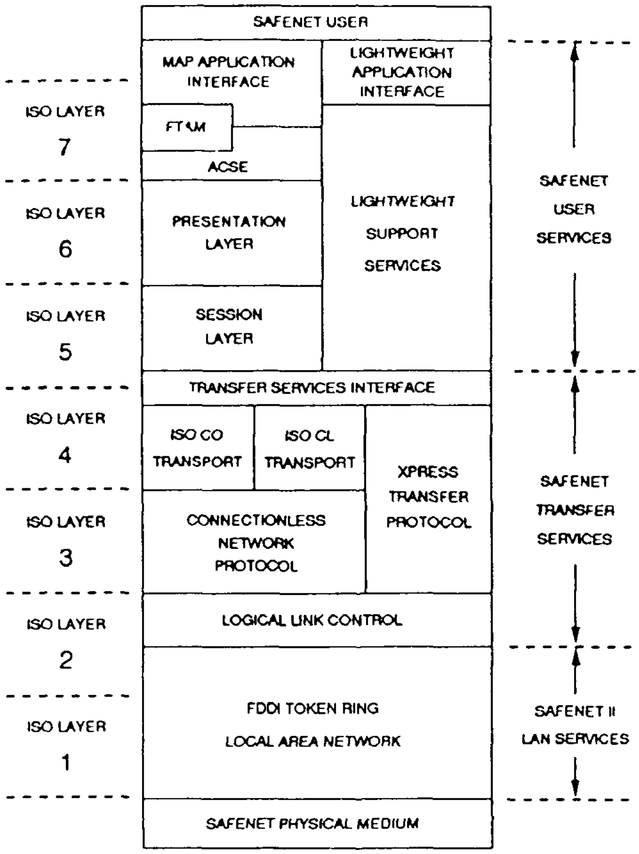

Figure 1. SAFENET II Protocol Profile

A second feature of the OSI suite is that it provides a network management capability in accordance with the MAP 3.0 standard. SAFENET II will extend these management mechanisms by providing object definitions for those protocols (such as FDDI) which are not included in the MAP specifications.

The OSI protocol suite is intended for situations where either the interoperability of independently developed SAFENET II nodes is a driving consideration, or the file handling capabilities of FTAM are required, or the system is of sufficient complexity that network management is required. While the OSI protocol suite provides these capabilities, it does so at the expense of increased data transfer latency and an inability to send the same data to multiple users simultaneously (i.e., multicast transfer).

3.2 Lightweight protocol suite

The lightweight protocol suite provides real-time data transfer to systems which require it. This suite includes a SAFENET-specific service definition for the lightweight support services which comprise the user services partition. These lightweight support services are intended to permit efficient access to the underlying transfer services, while providing additional functionality (e.g., directory services) as needed. They would be implemented to meet the specific requirements of a given system.

The transfer services in this suite include the Xpress Transfer Protocol (XTP)[11], which is being developed by Protocol Engines, Inc., and the ISO connectionless transport protocol[12]. XTP is particularly attractive to military real-time applications because it offers the promise of low-latency data transfer as well as multicast data transfer capabilities.

The lightweight protocol suite has no defined network management capability. If a system requires the performance of the lightweight suite along with network management support then the combined protocol suite should be used.

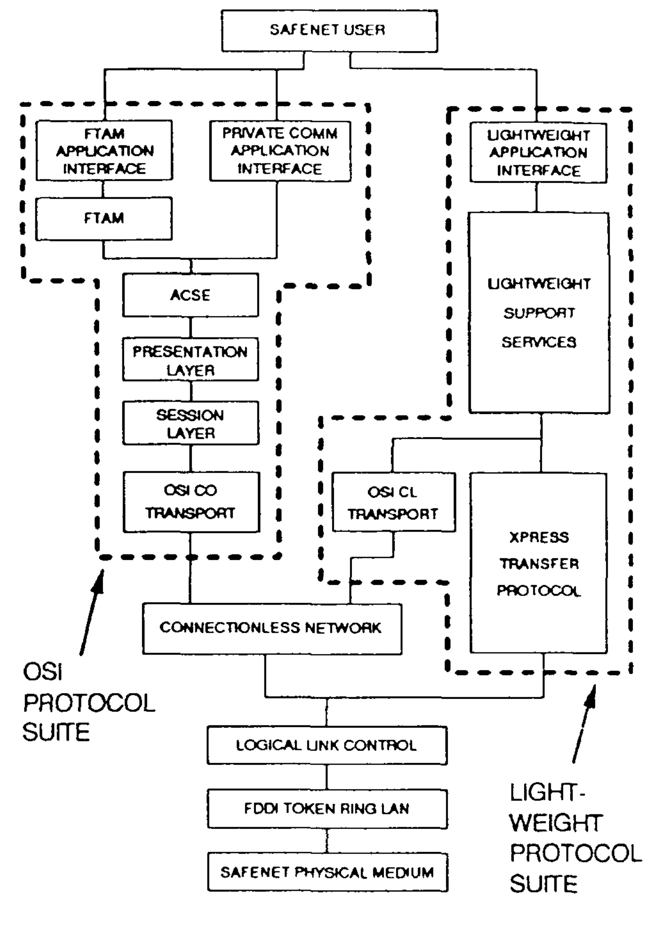

Figure 2. SAFENET II Protocol Suites

The lightweight protocol suite is intended for situations where either data transfer latency is critical, or multicast data transfer is required. While the lightweight protocol suite provides these capabilities, it does so at the loss of the ISO standard protocols and network management mechanisms. Furthermore, since the lightweight protocol suite permits system specific implementation, interoperability is limited to those stations which have implemented identical lightweight suites.

3.3 Combined protocol suite

The combined protocol suite is the union of the OSI and lightweight protocol suites. Therefore, this suite includes the combined capabilities of those suites. In addition, this suite provides management support for the protocols which comprise the lightweight protocol suite. This is done through the use of object definitions which are being developed by the SAFENET working group.

The combined protocol suite is intended for situations where the capabilities of both the OSI and lightweight protocol suites are required. The robust functionality of the combined protocol suite comes at the expense of the complexity of the system and the cost of its development.

3.4 Services common to all suites

There are several features which are common to all three protocol suites. Foremost among these is the FDDI local area network itself. This common LAN protocol permits SAFENET II station with different protocol suites to effectively coexist on the same network, even if their attached users can't interoperate. Thus, it is possible for unrelated systems (e.g., an administrative system and a combat system) to use the same SAFENET II network for their separate interconnection needs, provided their combined bandwidth requirements were not excessive.

Other protocols common to all suites include the IEEE 802.2 Logical Link Control protocol (LLC)[13] and the ISO connectionless network protocol (CLNP)[14]. The LLC protocol serves to direct the LAN packets to the correct network layer protocol: XTP or CLNP. CLNP is common to all suites because it provides network layer services to TP4 (in the OSI suite) and the ISO connectionless transport protocol (in the lightweight suite).

Another service common to all SAFENET II networks is the Global Time service. This is a service defined by SAFENET II which is intended to synchronize time-of-day information throughout the network. This ability to have concurrent time information is required by many Navy combat systems. The Global Time service provides a service definition which details how an application can read, write, and manage this time information. It also specifies that the Network Time Protocol (NTP)[15], currently running on the Internet, shall be used to support this service. Time synchronization remains an active area of investigation by the SAFENET working group.

4. PHYSICAL TOPOLOGY

The SAFENET II physical topology is based on the dual counter-rotating ring architecture inherent in FDDI. This physical topology is shown in Figure 3. The SAFENET II physical topology is designed to provide the high degree of reliability, flexibility, and survivability required for Navy mission critical computer systems.

The critical element in this topology is the trunk coupling unit (TCU). This is a device which enables a station to insert onto or remove itself from a network ring. For SAFENET II, the TCU is a 2x2 optical bypass switch, which is controlled by an electrical signal from the attached station. The TCU provides the ability to readily isolate a failed station from the network, thereby contributing to system reliability. The electrical control operates such that any loss of power to the station will result in the immediate isolation (known as bypassing) of that station. Additionally, the TCU can be dynamically controlled by the station to perform self-testing in response to apparent error conditions. These TCU control mechanisms are provided for in the FDDI standards.

4.1 Network layout

As shown, each network ring is comprised of a series of TCUs and connecting trunk cables. The primary and secondary ring trunk cables are intended to be located apart from each other to avoid simultaneous damage to both rings. This independent routing of the two rings is different from expected commercial FDDI practice, but it is not incompatible with the FDDI standard. The maximum trunk cable run permitted in SAFENET II is 200 meters. This distance is considered sufficient for almost any shipboard installation.

Each station attaches to a TCU via an optical interface cable and an electrical interface cable. A TCU and an attached station are intended to be located apart from each other to avoid simultaneous damage to both the station and the ring. The remote location of TCUs is different from suggested FDDI practice, but as before it is not incompatible with the standard. The maximum interface cable run, either optical or electrical, permitted in SAFENET II is 100 meters. This distance may seem very large for such an interface, but it is intended to provide maximum installation flexibility to the system integrator.

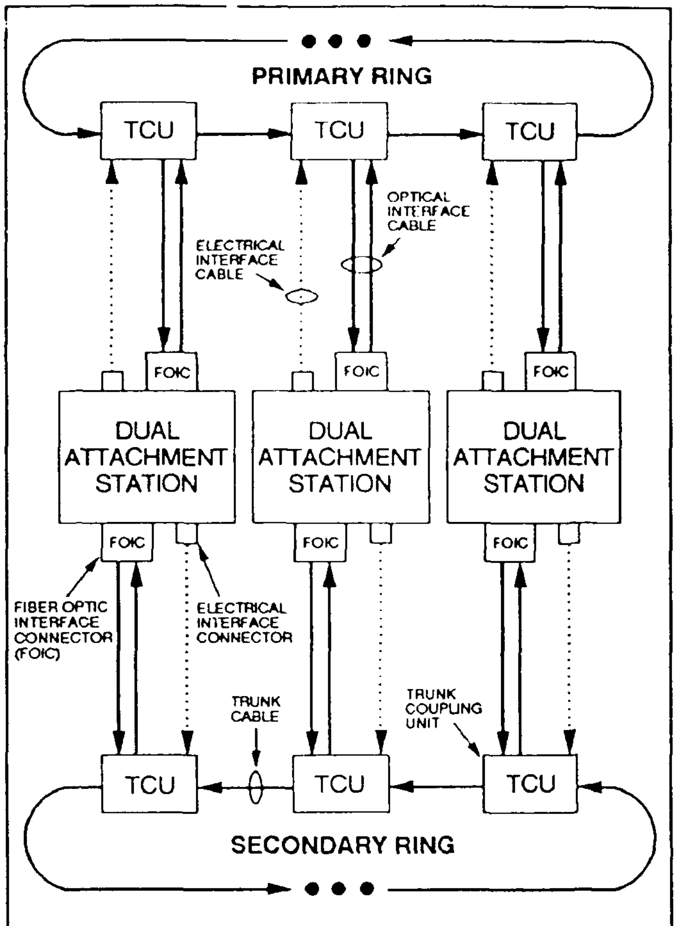

Figure 3. SAFENET II Physical Topology

4.2 Survivability

The SAFENET II standard includes survivability features as a result of the dual counter-rotating ring FDDI LAN upon which it is based. The FDDI standard provides for automatic reconfiguration upon the detection of a hard fault (such as a cable break). In SAFENET II, the FDDI optional hold policy will be used to provide a ring-switching capability, with wrap being used as a back-up method. Switching rings (i.e., moving all data transfers from the primary ring to the secondary ring) supports the independent routing of the primary and secondary rings and provides true transmission path redundancy. Only the use of redundant transmission paths will meet the survivability requirements of mission critical combat systems. These FDDI reconfiguration mechanisms are an area of active research within the SAFENET working group.

SAFENET II provides additional survivability by requiring each station to insert onto a ring by way of a trunk coupling unit (TCU). As described above, this permits the automatic bypassing of failed (or destroyed) stations from the network. The SAFENET II power budget, optical signal parameters, and fiber optic component specifications were developed such that a station would always be capable of transmitting data to a receiving station past at least five consecutive bypassed stations.

The SAFENET II topology also provides survivability by permitting the key network components to be located apart from each other. The trunk coupling units can be located away from their attached stations, and the cables comprising the two network rings can be routed independently through the ship. These features allow the network and its attached stations to absorb some damage without the entire system losing its ability to operate.

5. CONCLUSION

The SAFENET program has been successful in defining a set of network profiles which will meet the requirements of Navy shipboard combat systems. In particular, the SAFENET II standard provides the Navy with many advantages over current interconnection methods, including use of fiber optics, enhanced system survivability, and use of commercial standards. Further work is continuing in some areas of the SAFENET II standard, including time synchronization, reconfiguration mechanisms, network management object definitions, and multicast data transfer. It is expected that SAFENET II will meet the data communication requirements of a wide range of Navy computer-based systems, both now and in the future.

6. REFERENCES

1. D. T. Green and D. T. Marlow, "SAFENET - A LAN for Navy Mission Critical Systems", Proc. 14th Conf. Local Computer Networks, Minneapolis, MN, Oct 1989, pp. 340-346

2. IEEE 802.5, "Token Ring Access Method and Physical Layer Specifications", 1989

3. ISO 9314-1, "Information processing systems - Fibre Distributed Data Interface (FDDI) - Part 1: Token Ring Physical Layer Protocol (PHY)"

4. ISO 9314-2, "Information processing systems - Fibre Distributed Data Interface (FDDI) - Part 2: Token Ring Media Access Control (MAC)"

5. ISO 9314-3, "Information processing systems - Fibre Distributed Data Interface (FDDI) - Part 3: Token Ring Physical Layer, Medium Dependent (PMD)"

6. ANSI X3T9.5/84-49, "Fiber Distributed Data Interface - Station Management (SMT)", Draft proposed American National Standard

7. ISO 7498, "Information processing systems - Open Systems Interconnection - Basic Reference Model", 1984

8. H. Zimmerman, "OSI Reference Model - The OSI Model of Architecture for Open Systems Interconnection", IEEE Trans. on Comm., V. COM-28, N. 4, pp. 425-432, Apr 1980

9. MAP 3.0, "Manufacturing Automation Protocol Specification - Version 3.0", North American MAP/TOP Users Group, Aug 1988

10. ISO 8073, "Information processing systems - Open Systems Interconnection - Connection oriented transport protocol specification", 1986

11. XTP 3.4, "Xpress Transfer Protocol Definition - Revision 3.4", Protocol Engines Inc., Jul 1989

12. ISO 8602, "Information processing systems - Open Systems Interconnection - Protocol for providing the connectionless-mode transport service", 1987

13. IEEE 802.2, "Logical Link Control", 1985

14. ISO 8473, "Information processing systems - Data communications - Protocol for providing the connectionless-mode network service", 1988

15. D. L. Mills, "Network Time Protocol (Version 2) - Specification and Implementation", RFC 1119, Sep 1989

To be presented at:

SPIE OE/Fibers '90
San Jose, CA September 16-21, 1990